

# Corrigir erros de exibição de página EUN em SWA para solicitações HTTPS explícitas

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Problema](#)

[Solução](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve o problema de páginas EUN serem exibidas incorretamente no Cisco SWA para solicitações HTTPS explícitas.

## Pré-requisitos

### Requisitos

As informações neste documento supõem que:

- O Secure Web Appliance (SWA) é implantado no modo Explícito.
- O SWA está sendo executado nas versões 7.7.0 e anteriores.
- As solicitações HTTPS são bloqueadas, avisadas ou exigem confirmação do usuário.
- A Descriptografia HTTPS está habilitada.

### Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Problema

As páginas Aviso, Confirmação ou Notificação de usuário final (EUN) não são exibidas corretamente para solicitações HTTPS explícitas. O navegador exibe uma página de notificação

incompleta ou não exibe a página e, em vez disso, exibe uma página de erro.

Há vários problemas que cercam essas páginas quando você usa solicitações HTTPS explícitas. Quando você configura seu navegador para usar um proxy, o tráfego HTTPS é direcionado para o SWA sobre HTTP. Esta solicitação está formatada como um HTTPS sobre HTTP.

Há dois problemas conhecidos com navegadores que não tratam corretamente as respostas HTTP que o SWA retorna para solicitações HTTPS explícitas:

1. Quando uma solicitação HTTPS explícita é bloqueada, avisada ou exige confirmação do usuário, o SWA retorna um código de status HTTP/403.
2. Nessa resposta, o SWA inclui o conteúdo de notificação que normalmente deve ser renderizado na tela para que seja visível. No entanto, em alguns casos, o navegador não consegue entender a resposta dentro do conteúdo retornado.

Este é o comportamento do navegador que é observado:

- Quando o Internet Explorer Versão 6 (IE6) e algumas versões do IE7 são usados, essas solicitações não conseguem renderizar o conteúdo completo da resposta HTML. O navegador só honra os primeiros bytes (o conteúdo dentro do primeiro pacote) e ignora o resto. Nesses casos, você verá uma página incompleta que exibe apenas alguns caracteres.



Note: Se esse for o caso, a Cisco recomenda que você reduza a página de notificação padrão da resposta SWA. Para obter mais informações sobre como editar sua página EUN, consulte a seção Edição direta dos arquivos HTML da página de notificação do Guia do usuário do SWA.

---

- Quando o IE8 e versões mais recentes do Mozilla Firefox Release 3 são usados, o navegador ignora completamente a resposta que o SWA retorna e a mascara com sua própria página de erro. Esse comportamento do navegador anula a finalidade da notificação 403 e causa interrupções com o recurso.

## Solução

Esta seção descreve o processo que ocorre quando a Criptografia HTTPS está habilitada no SWA. Esse problema foi resolvido no SWA versão 7.7.0-500 e posterior (ID de bug da Cisco CSCzv25138) Como uma solução alternativa para o problema descrito anteriormente, use as informações fornecidas para garantir que seu sistema seja configurado de acordo.

Aqui está um exemplo do fluxo de tráfego quando uma solicitação HTTPS explícita é enviada:

- Quando a criptografia HTTPS está habilitada, o SWA primeiro valida a solicitação em relação às políticas de criptografia.
- Se a solicitação estiver marcada para PASSTHROUGH, o tráfego será permitido (sem aviso

ou EUN).

- Se a solicitação for marcada como DESCRIPTOGRAFADA, ela será validada de acordo com as políticas de Acesso. Nesse caso, se a política de acesso estiver configurada para AVISAR ou BLOQUEAR, a página EUN será exibida corretamente. Infelizmente, para Reconhecimento, o usuário deve navegar para a página HTTP e Reconhecer, o que exige a navegação pelo proxy e, em seguida, para o site HTTPS.
- O SWA lembra o endereço IP do cliente e não requer outra confirmação até que o temporizador expire.

## Informações Relacionadas

- [Guia do usuário do AsyncOS 14.5 para Cisco Secure Web Appliance - GD \(General Deployment\) - Cisco](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.